High Tunstall College of Science

Inspire | Support | Achieve

Protection of Biometric Information Policy

Revised	-	October 2023
Stakeholder Consulted	-	Admissions and Safeguarding Committee
Review Date	-	October 2024
Responsibility for Review	-	Senior Teacher Achievement and Standards, Senior ICT Technician

Contents:

Statement of intent

High Tunstall College of Science is committed to protecting the personal data of all its students and staff, this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. We will treat the data collected with appropriate care.

This policy outlines the procedure the college follows when collecting and processing biometric data.

1. [Updated] Legal framework

[Updated] This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- **[Updated]** DfE (2022) 'Protection of biometric information of children in schools and colleges'
- DfE (2018) 'Data protection: a toolkit for schools'.

This policy operates in conjunction with the following college policies:

- Data Protection Policy
- Records Management Policy
- Information Security Policy.

2. [Updated] Definitions

"Biometric data" is personal information, resulting from specific technical processing, about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, hand measurements, and voice. All biometric data is personal data.

An **"automated biometric recognition system"** is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (e.g., electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

"Processing biometric data" includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner
- Storing biometric information on a database
- Using biometric data as part of an electronic process, e.g., by comparing it with biometric information stored on a database to identify or recognise individuals.

"Special category data" is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, it is considered special category data.

[New] NOTE: The college does not use any surveillance system that utilise facial recognition, biometric or automated biometric recognition systems.

3. Roles and responsibilities

The governing body is responsible for reviewing this policy on an annual basis.

The headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO) is responsible for:

Monitoring the college's compliance with data protection legislation in relation to the use of biometric data.

Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the college's biometric system(s).

Being the first point of contact for the ICO and for individuals whose data is processed by the college and connected third parties.

The Data Controller is responsible for:

[New] Ensuring that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012.

[New] Identifying the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented.

[New] Ensuring that the processing of biometric data is done so in line with the school's Protection of Biometric Data Policy.

[New] The Compliance Officer role includes:

Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.

4. Data protection principles

The college processes all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. The college ensures biometric data is:

Processed lawfully, fairly and in a transparent manner.

Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As the data controller, the college is responsible for being able to demonstrate its compliance with the provisions outlined above.

5. Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

The Senior Teacher (Achievement and Standards) will oversee and monitor the process of carrying out the DPIA.

The DPIA will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks
- Be reviewed frequently and kept updated.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

The ICO will provide the college with a written response (within eight [8] weeks or fourteen [14] weeks in complex cases) advising whether the risks are acceptable, or whether the college needs to take further action. In some cases, the ICO may advise

the college to not carry out the processing. The college will adhere to any advice from the ICO.

6. Notification and consent

Please note: The obligation to obtain consent for the processing of biometric information of children under the age of eighteen (18) is not imposed by the Data Protection Act 2018 or the UK GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

Where the college uses students' biometric data as part of an automated biometric recognition system (e.g., using students' fingerprints to receive college dinners instead of paying with cash), the college will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing a student's biometric data, the college will send the student's parents a SIMS data entry form which requests biometric consent. Written consent will be sought from at least one parent/carer of the student before the college collects or uses a student's biometric data.

The name and contact details of the student's parents will be taken from the college's management information system (MIS). Where the name of only one (1) parent is included on the MIS, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The college does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g., their whereabouts or identity is not known
- The parent lacks the mental capacity to object or consent
- The welfare of the student requires that a particular parent is not contacted, e.g., where a student has been separated from an abusive parent who must not be informed of the student's whereabouts
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a student can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a student is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified, and their written consent obtained

- If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric data can be processed.

Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- How the data will be stored
- The parent's and the student's right to refuse or withdraw their consent
- The college's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

The college will not process the biometric data of a student under the age of 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent or carer has consented in writing to the processing
- A parent has objected in writing to such processing, even if another parent has given written consent

Parents and students can object to participation in the college's biometric system(s) or withdraw their consent at any time, and that if they do this, the college will provide them with an alternative method of accessing the relevant services.

Students will be informed that they can object or refuse to allow their biometric data to be collected and used via a SIMS data collection form upon their admission.

Where a student or their parents object, any biometric data relating to the student that has already been captured will be deleted.

If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the college will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s).

Where staff members or other adults use the college's biometric system(s), consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the college's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the college's biometric system(s), in line with alternative arrangements section of this policy.

7. Alternative arrangements

Parents, students, staff members and other relevant adults have the right to not take part in the college's biometric system(s).

Where an individual objects to taking part in the college's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g., where a biometric system uses fingerprints to pay for college meals, all individuals will be able to use a card for the transaction instead.

Also, where the biometric system uses fingerprints to use the print solutions, staff and students are able to log in, instead using a code or their username and password.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the student's parents, where relevant).

8. Storage and data retention

Biometric data will be managed and retained in line with the college's Records Management Policy.

The college will only store and process biometric information for the purpose for which it was originally obtained, and consent provides.

If an individual (or a student's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the college's system.

9. Security and breaches

The outcome of the DPIA will be used to identify the security measures that will be put in place to protect any unlawful and/or unauthorised access to the biometric data stored by the college.

These security measures and the process that will be followed if there is a breach to the college's biometric systems are outlined in the college's Information Security Policy and Information Security Incident Reporting Policy.

10. Monitoring and review

The governing body will review this policy on an annual basis. The next scheduled review date for this policy is October 2024.

Any changes made to this policy will be communicated to all staff, parents and students.